Claim Amendments:

1. (currently amended) A method comprising the steps of:

encrypting a data message m at a transmitter processor using a primary transmitter secret key z, wherein z is known to the transmitter processor but not to a receiver processor, to form a quantity E; ~~wherein El Gamal encryption is used for encrypting the data message m~~;

preparing a quadruplet (a_{new}, b_{new}, s_{new}, E) at the transmitter processor where:

$a_{new} = z^* y^c$ modulo p ;

$b_{new} = g^c$ modulo p;

s_{new} = signature $_c(a_{new}, b_{new}, E)$;

where $y = g^x$ modulo p, c is a random number ~~which is used in the step of encrypting the data message m using El Gamal encryption~~, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};

transmitting the quadruplet (a_{new}, b_{new}, s_{new}, E) from the transmitter processor to the receiver processor;

verifying the signature s_{new} at the receiver processor;

decrypting a_{new} and b_{new} at the receiver processor by using the receiver secret key x to get the primary transmitter secret key z;

using the primary transmitter secret key z to decrypt the quantity E and thereby obtaining the message m at the receiver processor.

2. (currently amended) The method of claim 1 and wherein:

the step of decrypting a_{new} and b_{new} at the receiver processor using the receiver secret key x to get the primary transmitter secret key z is comprised of computing $z = a_{new}/b_{new}^x$.

3. (cancelled)

4. (cancelled)

5. (currently amended) The method of claim 1 wherein:

the primary transmitter secret key z is determined at the transmitter processor from the formula of $z = g^{Y}$ modulo p, where Y is a random value chosen from the set [0..q], where q is a value picked using a known encryption method.

6. (currently amended) A method comprising the steps of:

creating a primary transmitter key z at a transmitter processor wherein the primary transmitter key is known to the transmitter processor but not to a receiver processor;

creating a secondary transmitter key z' at the transmitter processor wherein the secondary transmitter key is known to the transmitter processor but not to the receiver processor, wherein the secondary transmitter key z' ~~which~~ is a function of z;

encrypting a data message m , at the transmitter processor, using the secondary transmitter secret key z' to form a quantity E; ~~wherein El Gamal encryption is used for encrypting the data message m~~;

preparing a quadruplet (a_{new}, b_{new}, s_{new}, E) at the transmitter processor, where:

$a_{new} = z^{*} y^{c}$ modulo p ;

$b_{new} = g^{c}$ modulo p;

s_{new} = signature $_{c}(a_{new}, b_{new}, E)$;

where $y = g^{x}$ modulo p, c is a random number ~~which is used in the step of encrypting the data message m using El Gamal encryption~~, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c

that was used to determine a_{new} and b_{new};

transmitting the quadruplet (a_{new}, b_{new}, s_{new}, E) from the transmitter processor to the receiver processor;

verifying the signature s_{new} at the receiver processor;

decrypting a_{new} and b_{new} at the receiver processor, using the receiver secret key x to get the primary transmitter secret key z;

modifying the primary transmitter secret key z, at the receiver processor, to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to decrypt the quantity E and thereby obtaining the message m, at the receiver processor.

7. (original) The method of claim 6 and wherein:

the primary transmitter key z is provided which is not of the format used for producing the ciphertext E;

the secondary transmitter key z' is computed as a function of z, where the function is an arbitrary function.

8. (currently amended) A method comprising the steps of:

creating a primary transmitter key z at a transmitter processor;

creating a secondary transmitter key z' which is a function of z, at the transmitter processor;

providing a plurality of portion keys which are derived from the secondary transmitter key z', at the transmitter processor;

encrypting a data message m, at the transmitter processor, using the plurality of portion keys to form a quantity E~~, wherein El Gamal encryption is used for encrypting the data message m~~;

preparing a quadruplet (a_{new}, b_{new}, s_{new}, E) at the transmitter processor, where:

$a_{new} = z^* y^c$ modulo p ;

$b_{new} = g^c$ modulo p;

s_{new} = signature $_c(a_{new}, b_{new}, E)$;

where $y = g^x$ modulo p, c is a random number ~~which is used in the step of encrypting the data message m using El Gamal encryption~~, x is a receiver secret key of a receiver processor, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};

transmitting the quadruplet (a_{new}, b_{new}, s_{new}, E) from the transmitter processor to the receiver processor;

verifying the signature s_{new} at a the receiver processor;

decrypting a_{new} and b_{new}, at the receiver processor, using the receiver secret key x to get the primary transmitter secret key z;

modifying the primary transmitter secret key z, at the receiver processor, to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to determine the plurality of portion keys and using the plurality of portion keys to decrypt the quantity E and thereby obtaining the message m, at the receiver processor.

9. (previously presented) The method of claim 1 wherein

the signature s_{new} is determined by using a Schnorr signature method.

10. (previously presented) The method of claim 1 wherein

the signature s_{new} is determined using a Digital Signature Standard.

11. (currently amended) An apparatus comprising

a transmitter processor;

wherein the transmitter processor

encrypts a data message m using a primary transmitter secret key z, known to the transmitter processor but not known to a receiver processor, to form a quantity E; ~~wherein El Gamal encryption is used to encrypt the data message m~~; and

prepares a quadruplet (a_{new}, b_{new}, s_{new}, E) where:

$a_{new} = z^* y^c$ modulo p ;

$b_{new} = g^c$ modulo p;

s_{new} = signature $c(a_{new}, b_{new}, E)$;

where $y = g^x$ modulo p, c is a random number ~~which is used in the step of encrypting the data message m using El Gamal encryption~~, x is a receiver secret key of the receiver processor, and the parameters g, x, and p are picked using a known encryption method; and

wherein s_{new} is a signature, and wherein the transmitter processor determines s_{new} by using the same random number c that was used to determine a_{new} and b_{new}.

12. (cancelled).

13. (currently amended) The apparatus of claim 11 wherein

the transmitter processor uses a Schnorr signature method to determine s_{new}.

14. (currently amended) The apparatus of claim 11 wherein

the transmitter processor uses a Digital Signature Standard to determine s_{new}.

15. (new) The method of claim 1 wherein

El Gamal encryption is used for the encrypting steps.

16. (new) The method of claim 6 wherein

El Gamal encryption is used for the encrypting steps.

17. (new) The method of claim 8 wherein

El Gamal encryption is used for the encrypting steps.

18. (new) The apparatus of claim 11 wherein

El Gamal encryption is used for encrypting.